GA1.13: RCED-89-116

United States General Accounting Office

GAO

Report to the Chairman, Committee on Governmental Affairs, U.S. Senate

COMPLETED
41

June 1989

NUCLEAR NONPROLIFERATION

Better Controls Needed Over Weapons-Related Information and Technology

GAO/RCED-89-116

GAO

United States
General Accounting Office
Washington, D.C. 20548

Resources, Community, and
Economic Development Division

B-221179

June 19, 1989

The Honorable John Glenn, Chairman
Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

As requested, we examined the Department of Energy's controls over unclassified nuclear weapons information and technology developed at the agency's three weapons laboratories. On October 11, 1988, we provided you a related report on Energy's controls over foreign visitors—Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31).

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time, we will send copies of this report to appropriate congressional committees; the Secretary of Energy; and the Director, Office of Management and Budget. We will also make copies available to others upon request.

This work was performed under the direction of Keith O. Fultz, Director, Energy Issues. Other major contributors are listed in appendix II.

Sincerely yours,

J. Dexter Peach
Assistant Comptroller General

Executive Summary

Purpose

Since 1974, the United States has tried to limit proliferation by strengthening its controls over information and technology that could help other nations develop nuclear weapons. The major control mechanism—classification of weapons information—is designed to protect the most sensitive data. However, unclassified but potentially sensitive nuclear-related information and technology that have commercial uses are distributed throughout the world.

The Chairman, Senate Committee on Governmental Affairs, asked GAO to examine the Department of Energy's (DOE) controls over unclassified but sensitive information, which has commercial and nuclear weapons applications, developed at Lawrence Livermore National Laboratory, California, and Los Alamos National Laboratory and Sandia National Laboratories, New Mexico. The Chairman also asked GAO to obtain information on the types of nuclear-related hardware obtained by foreign countries.

Background

Various legislation requires DOE to both control and disseminate unclassified but potentially sensitive information. The Atomic Energy Act places controls over the transfer of unclassified nuclear information that could help weapons production. With the passage of the Nuclear Non-Proliferation Act and 1981 amendments to the Atomic Energy Act, the Congress further expressed its concern over the free flow of some unclassified information. In addition, in 1985 the Congress amended the Export Administration Act, emphasizing the need for controls over unclassified technologies that could significantly contribute to the military potential of other countries.

On the other hand, various technology transfer legislation requires DOE and the weapons laboratories to collaborate with the private sector to disseminate unclassified research results. Further, the Freedom of Information Act requires DOE to make most unclassified information available to anyone—domestic or foreign—who requests it, including data that the private sector could not export without a license from the Department of Commerce or authorization from DOE. Generally, DOE is not required to obtain prior authorization before transferring nuclear information or technology to foreign countries. (See ch. 1.)

Results in Brief

DOE has taken some actions to implement a 1981 congressional mandate to limit the dissemination of unclassified information related to atomic

defense activities. Nevertheless, sensitive countries—communist-controlled nations, countries suspected of developing nuclear weapons, or those viewed as a national security risk—have obtained information dealing with detonators, explosives, and firing sets that could assist or enhance nuclear weapons development. Foreign nationals obtain some information directly from DOE's weapons laboratories; DOE does not require the laboratories to track these requests. DOE recognizes that continuing to disseminate some unclassified information raises questions about its compliance with U.S. nonproliferation policy and in January 1989 issued internal guidance to identify data that should not be distributed to proliferation-risk countries.

Further, sensitive countries have obtained hardware that has both commercial and weapons-related uses. Twelve sensitive countries submitted about 1,160 export requests in calendar year 1987 for such hardware; all but 23 of the requests were approved. At least 290 of the approved requests were destined for facilities in countries suspected of conducting nuclear weapons activities.

Principal Findings

Proliferation-Risk Countries Receive Unclassified Sensitive Information

Each year DOE's weapons laboratories produce thousands of unclassified reports related to nuclear weapons research, development, and testing. In 1986 and 1987, for example, DOE produced about 39,000 reports and made over 60 percent available to the public through a government distribution center. DOE placed distribution restrictions on the others. From 1,000 reports, GAO judgmentally selected 30 and found that 68 percent of the recipients between January 1987 and April 1988 were from overseas. Sensitive countries—Iraq, Israel, and Pakistan—requested six of the same reports. One report discussed methods to improve a detonator that is used in most U.S. nuclear weapons; another described methods to shape the explosives used in these weapons.

In addition, the three laboratories respond to thousands of data requests. Between October 1985 and December 1987, they recorded more than 2,000 requests and honored almost 1,700. They did not honor the others primarily because the laboratory had no record of the information requested. Although the laboratories have some data on the number of requests, the information may not be complete because DOE does not require them to track the requests or information provided. In

1986 Sandia developed a system to track direct requests; Los Alamos began to provide information to Sandia in August 1988. Livermore does not have a system similar to Sandia's. Therefore, DOE has no systematic method to determine the information that may be needed or obtained by proliferation-risk countries.

Further, some of the information may have been considered sensitive under legislation passed in 1981. DOE issued regulations in 1985 and some guidance in 1988 to identify "Unclassified Controlled Nuclear Information" related in part to the design, manufacture, or use of nuclear weapons and restrict its distribution as the act required. DOE has not issued other guidance for the laboratories to identify information in a specific technology or programmatic area that meets the act's criteria. In the interim, according to Los Alamos and Sandia officials, they may have provided such information to sensitive countries. (See ch. 3.)

Certain Export Requirements Do Not Apply to DOE

Although substantial controls exist over the private sector's export of nuclear-related technology and information, DOE is generally exempt from these controls. In November 1988 DOE circulated a draft order for comment that would require DOE field offices and laboratories to identify and mark information that would be subject to export controls if the data had been developed by the private sector. Further, in January 1989, Defense Programs, the office responsible for overseeing the activities of the weapons laboratories, issued guidelines for the field offices and laboratories to use until a final order is approved. Defense Programs took this action to ensure that DOE complies with the Nuclear Non-Proliferation Treaty, which prohibits direct or indirect assistance in nuclear weapons development.

However, some within DOE have questioned its authority to restrict dissemination of unclassified information without specific legislation exempting "export controlled information" from Freedom of Information Act requests. Recognizing that statutory authority may be needed, Defense Programs asked DOE's General Counsel to seek a Freedom of Information exemption for unclassified data that has military or space applications. DOE's Deputy General Counsel expects to respond to Defense Programs by July 1989. (See ch. 3.)

Nuclear-Related Hardware Exported to Sensitive Countries

In addition to obtaining DOE information, sensitive countries routinely obtain hardware from the United States that has both nuclear weapons and commercial applications (dual use). In calendar year 1987, 12 sensitive countries submitted about 1,160 export requests for more than 65,000 dual-use items; all but 23 requests (about 10,420 items) were approved. Although the hardware has commercial uses and most of the export requests stated those purposes, four countries received items that could benefit their weapons development activities and about 290 of the approved requests were destined for facilities suspected of conducting nuclear weapons development activities. According to Defense Programs officials, the hardware has many commercial uses, and it is neither practical nor feasible to completely restrict their export, but they plan to periodically provide the Department of Commerce information on emerging technologies that warrant greater scrutiny before export licenses are approved.

Since dual-use hardware can also be obtained from other countries, DOE recognizes that U.S. controls are effective only when other suppliers also limit their export. Currently, no multilateral program exists to control the international flow of technology that could help a proliferation-risk country develop or manufacture a nuclear weapon. As a result, DOE has been working with various international organizations to control the transfer of technology and components that can be used in nuclear weapons. (See ch. 2.)

Recommendations

To help minimize the risks associated with releasing unclassified nuclear weapons-related information and better protect national security, GAO recommends, in part, that the Secretary of Energy

- require the laboratories to track foreign requests for information and institute effective oversight measures to ensure that they do so,
- issue guidance to the weapons laboratories for use in identifying and limiting the dissemination of "Unclassified Controlled Nuclear Information" in accordance with the 1981 congressional mandate, and
- seek a legislative exemption from the Freedom of Information Act for data categorized by DOE as export controlled information.

Agency Comments

GAO discussed the facts in this report with DOE headquarters and laboratory officials. They generally agreed with the facts but offered some clarifications that were incorporated where appropriate. As requested, GAO did not ask DOE to comment officially on this report.

Contents

Executive Summary		2
Chapter 1 Introduction		8
	DOE Is Faced With Conflicting Legislation	8
	DOE's Organization for Managing Technology Transfer and Security	10
	U.S. Controls Over Exports	11
	Objective, Scope, and Methodology	12
Chapter 2 Security-Risk Countries Obtain Information and Hardware That Could Help Develop Weapons		16
	Nuclear-Related Information Obtained by Proliferation-Risk Countries	16
	Dual-Use Hardware Exported to Sensitive Countries	24
Chapter 3 DOE Efforts to Limit Information Dissemination		26
	DOE Has Not Yet Implemented UCNI Controls	26
	DOE Has Developed Export Control Guidelines	29
Chapter 4 Conclusions and Recommendations		33
	Free Flow of Information May Endanger National Security	33
	Program Weaknesses	33
	Conclusions	34
	Recommendations to the Secretary of Energy	35
Appendixes		
	Appendix I: Activities Conducted at DOE's Nuclear Weapons Laboratories	38
	Appendix II: Major Contributors to This Report	39
Tables		
	Table 2.1: Foreign Purchasers of 30 DOE Documents From NTIS	18
	Table 2.2: Foreign Purchasers of Five-Selected Computer Codes	21

Table 2.3: Requests for Information From Communist Countries—October 1985 to December 1987 23
Table 2.4: Requests for Information From Other Sensitive Countries—October 1985 to December 1987 24

Abbreviations

DOE	Department of Energy
GAO	General Accounting Office
NESC	National Energy Software Center
NTIS	National Technical Information Service
OSTI	Office of Scientific and Technical Information
UCNI	Unclassified Controlled Nuclear Information

Introduction

Since World War II, the United States has been confronted with the dilemma of promoting nuclear technology transfer for peaceful purposes while restricting the flow of unclassified sensitive information that could compromise national security. However, international proliferation developments, such as India's explosion of a "peaceful" nuclear device in 1974, and recently published reports of Israel's nuclear arsenal, Pakistan's nuclear weapons capability, and the possibility that these and other nations try to obtain information and technology from the United States, have influenced many in the Congress and the administration to advocate tighter controls over the release of unclassified but potentially sensitive information. At the same time, others in the Congress and the administration are seeking to accelerate the transfer of federally funded technology to the private sector to forestall the erosion of U.S. technological leadership and enhance the industrial competitiveness of the United States in the world marketplace.

The Department of Energy (DOE) conducts the nation's program to design, test, and produce nuclear weapons. DOE owns 9 multiprogram and about 30 specialized laboratories (most are contractor operated) to carry out this mission. DOE facilities perform all aspects of nuclear weapon design and construction, from basic research performed at three facilities—Lawrence Livermore National Laboratory, California, and Los Alamos National Laboratory and Sandia National Laboratories, New Mexico—to weapons assembly performed at various facilities. However, DOE also conducts unclassified activities at these laboratories, such as solar energy research. (Appendix I briefly describes the activities conducted at the laboratories.)

DOE Is Faced With Conflicting Legislation

Under the Atomic Energy Act, DOE controls the dissemination of nuclear information to protect the national defense and security. In accordance with this responsibility, DOE classifies the most sensitive information and limits its distribution to U.S. citizens holding proper security clearances and having a "need to know" the details of the information or technology. However, the act also established a policy to promote the peaceful uses of nuclear energy and encouraged the United States to assist foreign countries in unclassified nuclear research and commercialization.

From the mid-1950s to the mid-1970s, the United States relied primarily on political commitments and international safeguards to control nuclear proliferation. However, India's 1974 explosion of a nuclear device caused the United States to reassess its nonproliferation controls

because the plutonium used in the explosion may have been produced, albeit indirectly, with U.S. assistance. To reduce the risk of further proliferation, the Congress enacted the Nuclear Non-Proliferation Act of 1978, which provided stronger controls over the export of U.S. nuclear technology. For example, the act requires the Secretary of Energy to authorize the private sector's export of technology and know-how to build and operate nuclear facilities. The Congress wanted to provide greater assurance against the diversion of materials and technology essential to the creation of, or the ability to create, nuclear weapons.

However, because some information or technology developed by DOE has both nuclear weapons and commercial applications (dual use), other legislation requires DOE and the weapons laboratories to collaborate with the private sector to disseminate unclassified research results. For example, the Stevenson-Wydler Technology Innovation Act of 1980 and the Federal Technology Transfer Act of 1986 promote commercialization of unclassified technology. Stevenson-Wydler also requires all DOE laboratories to establish Research and Technology Applications Offices to promote the transfer of federally funded technology to state and local governments and the private sector, while the Technology Transfer Act enhances the competitive position of U.S. industry in foreign markets through reduced government export controls. In addition, under the Freedom of Information Act, DOE must make all government information available to anyone who requests it unless the information is exempt under the act. For example, classified and unclassified controlled nuclear information (UCNI) are exempt. Therefore, DOE must effectively manage and control weapons-related information and technology but make available unclassified information and technology that has trade value or commercial uses.

However, some unclassified DOE information and technology may be useful to nations seeking to develop or advance their nuclear weapons research, development, and production programs. For example, some believe that the United States indirectly assisted India to develop its nuclear device through the liberal publication of reprocessing data. In addition, according to 1984 and 1985 DOE studies, information on classified programs can be derived from publicly available unclassified data. Further, according to a DOE export control official, foreign nations obtain unclassified information published by specific individuals who work in sensitive areas at DOE's weapons laboratories.

DOE's Organization for Managing Technology Transfer and Security

Within DOE several organizations share responsibility for implementing the Department's technology transfer and security programs. The key participants and their roles are summarized below.

- The Assistant Secretary for Defense Programs is responsible for managing the activities conducted at the three weapons laboratories, as provided in DOE Order 5600.1 (Management of the Department of Energy Weapon Program and Weapon Complex, June 27, 1979). Also, the Assistant Secretary, under DOE Orders 5650.3 (Identification of Unclassified Controlled Nuclear Information, Feb. 29, 1988) and 5635.4 (Protection of Unclassified Controlled Nuclear Information, Feb. 3, 1988), is required to provide guidance to DOE field offices and laboratories to identify and control certain sensitive, unclassified information.
- The Assistant Secretary for Management and Administration has overall responsibility for DOE's scientific and technical information management program. Under the Assistant Secretary, the Director of Administration is responsible for implementing DOE Orders 1430.1A (Managing Scientific and Technical Information, Sept. 10, 1986) and 1430.2A (Scientific and Technical Information Program, Dec. 14, 1987) regarding the operation of the Office of Scientific and Technical Information (OSTI) located in Oak Ridge, Tennessee—DOE's central facility for collecting and disseminating DOE-sponsored research and development information. OSTI is also responsible for providing unclassified reports to the Department of Commerce's National Technical Information Service (NTIS) for public dissemination.

  The Director of Administration also oversees the operation of the National Energy Software Center (NESC) in Argonne, Illinois—DOE's central facility for collecting and disseminating computer software—as provided in DOE Order 1360.4A (Scientific and Technical Computer Software, Oct. 17, 1987).

- The Office of Energy Research, which reports to the Under Secretary, manages the Research and Development Technology Transfer Program under DOE Order 5800.1 (Research and Development Laboratory Technology Transfer Program, Mar. 25, 1982).

DOE headquarters also delegates significant aspects of program implementation to the field offices with oversight responsibility for the weapons laboratories. Both the San Francisco Operations Office—which is responsible for Livermore—and the Albuquerque Operations Office—which oversees both Los Alamos and Sandia—are responsible for day-

to-day program management and contract administration at the laboratories. The operations offices also oversee the activities of technology transfer programs at the laboratories and are responsible for ensuring that the laboratories provide copies of DOE-sponsored scientific and technical information to OSTI and computer software to NESC.

In addition, DOE's operations offices have delegated certain responsibilities to the contractors that operate the laboratories. For example, the laboratories, using DOE-approved guidelines, determine the classification of the documents they produce and ensure that laboratory personnel who publish or provide papers at conferences are advised about the potential dangers in the discussions that follow the presentations. In addition, the laboratories have established technology transfer programs to identify products and ideas that have commercialization potential, coordinate industry visits, and respond to information requests.

U.S. Controls Over Exports

Under the Atomic Energy Act, as amended by the Nuclear Non-Proliferation Act, and the Export Administration Act, certain nuclear-related assistance provided to foreign countries must be approved by various federal organizations depending on the type of assistance—hardware or technical information. The Nuclear Regulatory Commission and the Department of Commerce license the exports of commercial nuclear facilities, components, and other hardware. Dual-use hardware must receive a Commerce export license; DOE reviews the export requests before Commerce issues a license.

To help Commerce carry out its responsibilities, DOE developed the Nuclear Referral List, which enumerates dual-use hardware that is controlled for nonproliferation reasons and require DOE's review prior to export. Commerce has incorporated the Nuclear Referral List into its list of hardware and technologies that require an export license (Commodity Control List, part 779, export administration regulations). In addition, Defense Programs developed the Nuclear Proliferation Watch List, which identifies facilities and organizations in certain countries suspected of conducting nuclear weapons activities. DOE developed this list for Commerce to use in referring export cases to DOE. DOE reviews the cases in detail to ensure they are not contrary to U.S. nonproliferation policy or detrimental to the interests of the United States. All potentially high-risk exports—including technical information—to the facilities or organizations identified in the list are to be reviewed to ensure that they do not represent a proliferation risk.

In addition, under the Arms Export Control Act of 1976, as amended, the Department of State licenses the export of arms, munitions, and related technical data in consultation with appropriate executive branch agencies. Within State, the Office of Munitions Control carries out these responsibilities under the International Traffic in Arms Regulations. The regulations include several categories of nuclear-related equipment, materials, or technology. State is required to refer export applications for these items to DOE for its review. In a September 1987 report, we found a number of weaknesses in State's application review process.[1] For example, State did not routinely check export license application data and rarely requested assistance from U.S. embassies to verify the foreign purchasers. In addition, State did not systematically check to determine whether the applicant had previously been denied export privileges by Commerce, nor did State seek information from other government agencies that maintain information on export violators.

To facilitate the interagency processing of export license applications, a number of groups have been formed. For example, the Subgroup on Nuclear Export Coordination was established to serve as a forum for exchanging and coordinating agency views. Representatives from the Departments of State, Energy, Commerce, and Defense, the Arms Control and Disarmament Agency, and the Nuclear Regulatory Commission make up the group. The Subgroup serves as an advisory body in export decisions.

Objective, Scope, and Methodology

On July 10, 1987, the Chairman, Senate Committee on Governmental Affairs, asked us to examine DOE's controls over foreign visitors to the weapons laboratories and nuclear weapons information that could be useful to foreign nuclear weapons programs. On October 11, 1988, we issued the first report, Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31). This second report addresses DOE's controls over information and hardware that could be useful to proliferation-risk nations. On the basis of discussions with the Chairman's office, we agreed to issue an unclassified report. As a result, we cannot provide some information in its entirety.

To obtain an overall perspective on the legislation that requires DOE to control and disseminate information, we reviewed the Atomic Energy Act of 1954, Nuclear Non-Proliferation Act of 1978, Stevenson-Wydler

[1] Arms Exports: Licensing Reviews for Exporting Military Items Can Be Improved (GAO/NSIAD-87-211, Sept. 9, 1987).

Technology Innovation Act, and Federal Technology Transfer Act of 1986; past GAO reports dealing with NESC, State's Office of Munitions Control, and DOE's control over reprocessing information;[2] and a March 1988 Defense Programs study, Technology Security. We also reviewed DOE's internal policies contained in a number of DOE Orders (i.e., 5600.1, 5650.3, 1430.2A, and 1260.4A) and Los Alamos and Sandia guidance concerning the release of UCNI. Using this information, we assessed the adequacy of DOE's internal controls.[3]

In addition, we met with DOE headquarters, field office, and laboratory officials to discuss the policies and procedures used to review documents before they are made available for public distribution, the adequacy of DOE's guidance to implement UCNI's requirements, and the effectiveness of UCNI to safeguard sensitive, unclassified information. At DOE headquarters we met with officials in the Office of Management and Administration and Defense Programs' Office of Classification and Technology Policy; at the Albuquerque and San Francisco Operations Offices, with classification officials; at Los Alamos and Sandia, with classification and technology transfer officials; and at Livermore, with technology transfer officials.

To determine the types of information obtained by foreign countries, we obtained a list from OSTI on the publicly available technical reports produced by Livermore in 1987. OSTI records showed about 1,000 such reports. Because we judged this to be a sufficiently large database for our objectives, we did not obtain similar data for reports produced by Sandia and Los Alamos. To determine whether information in the 1,000 reports could benefit foreign nuclear weapons programs, we judgmentally selected 30 documents from 6 areas—nuclear explosives, chemical explosives, precision machining, components and materials for fusion technology, and microwave and laser technologies—related to weapons design, production, or testing. We also obtained OSTI officials' views on the adequacy of DOE's guidance to limit the distribution of this type of information.

[2]Software Distribution: Review of the Department of Energy's National Energy Software Center (GAO/IMTEC-88-2, Oct. 14, 1987), Arms Exports: Licensing Reviews for Exporting Military Items Can Be Improved (GAO/NSIAD-87-211, Sept. 9, 1987), and Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information (GAO/RCED-87-150, Aug. 17, 1987).

[3]Internal controls that federal agencies are required to follow are set forth in GAO's Standards for Internal Controls in the Federal Government, published in 1983 pursuant to the Federal Manager's Financial Integrity Act of 1982.

In addition, we obtained from NTIS a list of all foreign and domestic purchasers of the 30 documents. To further assess their availability, we conducted a library search at the University of Colorado, Boulder, Colorado (a government repository library), and contacted the U.S. Library of Congress. To determine the significance of the 30 documents, we selected 6 of those most frequently requested and asked classification officials in DOE's Albuquerque office whether they (1) fell in the UCNI category and (2) could help a nation develop nuclear weapons. We also obtained from NTIS a list of foreign purchasers who obtained DOE-generated data in six technology areas through a subscription method established by NTIS. The six areas included precision detonators, neutron generators, high explosives, streak and framing cameras, flash x-ray systems, and firing sets.

Further, we obtained information from NESC, Argonne, Illinois, about foreign requests for computer codes that were developed at the weapons laboratories[4] and discussed NESC's distribution controls with its officials. In addition, we selected five codes that officials from an intelligence agency said were obtained by communist or other sensitive countries because of their applicability to U.S. nuclear weapons research and development activities. At NESC, we obtained information on the purchasers of the five codes between October 1984 and June 1988.

We also obtained data, where available, on the number of "direct" requests to laboratory staff from foreign nationals and obtained the laboratories' views on DOE's and their policies and procedures as well as the possible national security implications of direct requests. Because of the manner in which the laboratories retain this information, we obtained Sandia and Los Alamos data for calendar years 1986 and 1987 and Livermore's data for fiscal years 1986 and 1987. Where we discuss this information in chapter 2, we refer to the time period as October 1985 to December 1987.

To determine the types of dual-use hardware that foreign nationals have sought, we obtained calendar year 1987 data—the most current at the time of our request—on export license applications and approvals for 12 sensitive countries in eight areas. The areas included neutron generators, streak and framing cameras, flash x-ray systems, digital oscilloscopes, calibration gauges, measuring equipment, particle accelerators, and electron video tubes. We selected these eight areas because they are

[4]As used in this report, computer codes refer to an entire computer program and major subprograms within it.

on Commerce's Commodity Control List and could help other countries in developing or advancing their nuclear weapons programs. However, we did not search DOE's files to ensure that the agency reviewed the export license requests.

We discussed the facts in this report with officials from Defense Programs' Office of Classification and Technology Policy, the Albuquerque Operations Office, Sandia, and Los Alamos. In addition, Defense Programs obtained input from a Livermore official on the facts applicable to that laboratory. Although the officials generally agreed with the facts presented, they offered some clarifications that were incorporated where appropriate. As requested, we did not ask DOE to review and comment officially on this report. Our work was performed between January 1988 and October 1988 in accordance with generally accepted government auditing standards.

Chapter 2

Security-Risk Countries Obtain Information and Hardware That Could Help Develop Weapons

DOE makes readily available a great deal of unclassified information and computer codes that could assist sensitive countries in developing or advancing their nuclear weapons programs.[1] As a result, sensitive countries—such as Iraq, India, and Pakistan—have obtained reports or computer codes that were developed by DOE's weapons laboratories. For example, between January 1987 and April 1988, communist and other sensitive countries received 193 documents in 6 particularly sensitive subject areas, such as high explosives and special cameras.

In addition, although DOE has procedures to control yet disseminate scientific and technical information, we found that the laboratories do not fully comply with the procedures established. For example, the laboratories do not send all computer codes to NESC for distribution. Further, DOE allows the laboratories to respond to requests for information and computer codes but does not require them to document these requests or accumulate data that could assist nonproliferation experts in determining the weapons development status and/or needs of various nations.

Further, foreign nationals from sensitive countries have received dual-use items, such as neutron generators and digital oscilloscopes. In calendar year 1987, 12 sensitive countries submitted about 1,160 export requests; all but 23 were approved. At least 290 of the approved requests were from facilities or organizations suspected of conducting nuclear weapons development activities.

Nuclear-Related Information Obtained by Proliferation-Risk Countries

DOE publishes thousands of unclassified reports related to nuclear weapons research, development, and testing. Some of this information could help foreign nations develop or enhance their nuclear weapons programs, according to DOE studies. We found that countries suspected of developing weapons—such as Israel and Pakistan—and others considered sensitive by DOE—such as Argentina, India, and South Africa—obtain reports concerning nuclear explosives and special cameras. In addition, sensitive countries have obtained computer codes developed by the weapons laboratories. Both the reports and codes have sometimes been obtained directly from laboratory personnel.

[1]DOE's policies identify 57 sensitive countries, including communist-controlled nations, countries suspected of developing nuclear weapons, and other nations viewed as a national security risk.

Unclassified Reports Distributed to Sensitive Countries

Under DOE Orders 1430.1A and 1430.2A, DOE makes unclassified nuclear-related research data developed by the weapons laboratories available to the scientific, technical, and industrial communities and the public through approved channels. The order requires the laboratories to review all reports, determine the appropriate distribution limitations for them, and send them to OSTI for further processing regardless of their classification. OSTI summarizes the unclassified reports, enters a synopsis of those without distribution restrictions in an energy database, and then sends most reports to NTIS, which is the central source for U.S. government-sponsored research, development, and engineering reports.

OSTI has no classification or review responsibilities for incoming reports. However, if OSTI notices a discrepancy between a laboratory's classification of a document and its understanding of applicable DOE policies, OSTI contacts the laboratory and/or responsible program office to resolve the issue. According to OSTI officials, each year they flag about 1 percent of the unclassified reports they review. However, the vast majority of reports sent to OSTI carry no distribution limitations and are disseminated on an unlimited basis.

In 1986 and 1987, for example, OSTI processed about 18,000 and 21,000 DOE reports, respectively. In both years, over 60 percent were available through NTIS; the remaining reports were not available for public dissemination because of various distribution restrictions. In addition, the energy database contains about 2 million references to reports, articles, books, and conference papers from around the world. Both domestic and international users can directly access the database. A March 1988 Defense Programs study stated that individuals from the Soviet Union routinely gain access to this and other commercial and government databases from which the user can retrieve in seconds technical data that would otherwise take months of painstaking library research.

Once OSTI sends the reports to NTIS, NTIS sells them either in printed form or on microfiche. In addition to selling individual documents, NTIS sells subscriptions for certain categories of information it has established. Subscribers receive all documents in each data category for which they have a subscription. NTIS sells this information to both foreign and domestic customers, as well as to government repositories, such as the Library of Congress, selected university libraries throughout the country, international libraries, and foreign embassies.

At our request, NTIS searched its records for foreign subscribers for six technologies that we selected. The technologies considered to be particularly sensitive included precision detonators, neutron generators, high explosives, streak and framing cameras, flash x-ray systems, and firing sets. Of the 34 foreign subscribers of this information, 11 were from sensitive countries, including the Peoples Republic of China, India, Iraq, and Argentina. We also selected 30 documents from the 6 technology categories. NTIS records show that the majority of purchasers were from foreign countries. For example, between January 1987 and April 1988, NTIS distributed 530 copies of the 30 documents. Of the total, 132 were sent to domestic addresses; 360 were sent overseas. On the basis of available information, we could not determine the type of recipients for the remaining 38 documents. Table 2.1 shows the foreign purchasers of the 30 documents from NTIS.

Table 2.1: Foreign Purchasers of 30 DOE Documents From NTIS

Countries	Number of reports obtained
Communist	
Bulgaria	2
Peoples Republic of China	71
Sensitive	
Argentina	5
India	12
Iraq	18
Israel	26
Kuwait	1
Pakistan	21
South Africa	5
South Korea	28
Taiwan	4
Other	
Australia	14
Canada	8
Federal Republic of Germany	25
Finland	16
France	24
Japan	19
New Zealand	7
Sweden	32
United Kingdom	22
Total	**360**

We found that Iraq, Israel, and Pakistan received the same six reports and Argentina and India received four of the six. On the basis of a review of abstracts of these reports, Albuquerque and Sandia classification officials told us that all six related to basic science but could help countries develop or advance their nuclear weapons program. For example, the reports contain information for

- modifying high explosives,
- improving ultrafast cameras that are used to study the effects of a nuclear detonation,
- improving a detonator that is used in most U.S. nuclear weapons,
- improving the understanding of high explosives,
- shaping and machining high explosives,
- setting off high explosives (this information could also be useful to saboteurs).

Subsequently, however, the Sandia official told us that, upon examination of the complete reports, he did not believe they would assist a country in developing nuclear weapons. In addition, a Los Alamos official does not believe that these documents would be useful to a nation with a weapons development program. The official pointed out that DOE and the laboratories have released for valid reasons far more useful and relevant material. The official acknowledged that information on high explosives would be of interest to a proliferation-risk nation, as would many other areas covered by laboratory publications.

Computer Codes Can Be Obtained by Sensitive Countries

In addition to obtaining research results and other information that DOE publishes, communist and other sensitive countries can obtain computer codes initially developed for the U.S. nuclear weapons program. The laboratories develop unclassified basic research and development computer codes as well as codes to model, design, and test nuclear weapons. Under DOE's procedures, unclassified codes resulting directly or indirectly from DOE-funded research must be submitted to NESC for distribution.

NESC sells the codes for $50 to $4,500 depending upon the size and complexity of the program, the costs to verify that the program will perform as advertised, and the type of recipient (nonprofit, commercial, or foreign). As of May 1988, NESC had about 1,460 computer codes, and about 870 were available to sensitive countries. However, the codes must be at least 2 years old before NESC will sell them to those countries. NESC takes this action to give domestic companies an advantage over foreign competitors. In addition, NESC flags each request from a sensitive country

and sends the request to Defense Programs for review before providing the code. According to Defense Programs officials, they consider the weapons development status of the country and the possible benefit that the code could provide toward furthering that status. During fiscal years 1986 and 1987, NESC honored 219 requests from foreign countries for computer codes. As of June 1988, Defense Programs had denied or was reviewing 27 requests from sensitive countries for 43 codes, including 6 requests for 7 codes from countries such as Iraq, Iran, and Pakistan.

According to Sandia and Los Alamos technology transfer officials, the laboratories do not submit all codes to NESC. A Sandia official estimated that the laboratory develops about a hundred codes annually, but NESC records show that the laboratory submitted only 16 during fiscal year 1987. In addition, available information shows that Livermore submitted 130 codes to NESC between fiscal years 1985 and 1988. According to Defense Programs officials, the laboratories send NESC only finished codes and subroutines that have complete documentation on their use.

For many codes NESC also sells the line-by-line input instructions. Both Sandia and Los Alamos officials said that knowledgeable individuals could, with minimal effort, input the information needed to help nations develop nuclear weapons. We obtained information on the foreign purchasers of five codes that had been developed by the weapons laboratories. The laboratories initially developed three of the codes to model: (1) material decay (ALICE), (2) two-dimensional studies of stress effects on components (DYNA2D), and (3) three-dimensional studies of stress effects on components (DYNA3D). DOE used the other two codes—NIKE2D and NIKE3D—to conduct structural analyses of gun-fired projectiles, stress analysis of nuclear weapons components, and precision-machining calculations.

Although the five codes were developed as part of this country's nuclear weapons program, they do have commercial applications. According to a Livermore document, the DYNA codes have been provided to about 500 domestic and foreign organizations, including automobile manufacturers, electric utilities, well-drilling firms, computer consulting companies, and other government agencies, such as the Nuclear Regulatory Commission. Further, Livermore has been working with domestic metal-forging companies using NIKE2D to predict final shapes, loads, and material damage. A Livermore document also states that the NIKE codes show great promise in reducing the time and cost to manufacture metal-forged products and improving product reliability and integrity.

Under DOE's order, a purchaser of codes from NESC must agree not to redistribute them without NESC's approval. However, NESC officials told us that DOE has no mechanism to enforce this requirement or determine whether a purchaser plans to redistribute a program or when a violation has occurred. For example, Japan began to market the DYNA3D program using pictures and research results taken from literature that Livermore had attached with the computer code. The pictures show an F-111 aircraft dropping a bomb by parachute onto a runway, and the accompanying report refers to, and shows pictures of, the distortion of the shock mitigator component when the bomb strikes the ground. The Japanese marketing brochure also provides the name of the Livermore official to contact for further information about the program.

In addition, a Livermore document states that ENEA, a computer program library in Italy, routinely distributes codes to other countries. According to Defense Programs officials, ENEA does not receive nuclear-related codes or software. They also pointed out that under international agreements, DOE exchanges nuclear-related computer software with other nations (about 75 requests were honored in fiscal years 1986 and 1987), and the recipient country agrees not to redistribute the codes.

Between October 1984 and June 1988, NESC received 20 foreign and 16 domestic requests for the five codes; Pakistan obtained two of them. Table 2.2 shows the foreign recipients of the five computer codes.

Table 2.2: Foreign Purchasers of Five-Selected Computer Codes

Code name	Foreign purchasers
ALICE	France
DYNA2D	Japan France Pakistan
DYNA3D	Japan Belgium France Pakistan
NIKE2D	France
NIKE3D	France Japan

According to Defense Programs officials, in late 1984 or early 1985, they instituted a process to review all sensitive country requests for codes. Since that time, Pakistan has not received any codes from NESC.

However, the information shown in table 2.2 very likely understates the number of codes that have been obtained by foreign countries. According to DOE field office and laboratory officials, foreign nationals frequently request codes directly from laboratory officials. The laboratories do not maintain records on the number of requests they receive, but Sandia keeps records of those that have been denied. Sandia records show that between September 1985 and March 1987 the laboratory denied a South African request for a non-nuclear-related code and referred the requester to NESC.

Foreign Nationals Obtain Information Directly From Laboratory Personnel

To facilitate the exchange of scientific and technical information, DOE's procedures (Orders 1430.1A and 1430.2A) allow laboratory staff to respond directly to requests for published information from foreign nationals—including those from countries considered sensitive by DOE. When the request is "routine," DOE allows the laboratories to send the information without prior approval, although the orders do not define a routine request.

The following two examples illustrate the types of requests received by the laboratories. Livermore received a December 1984 request from India's Bhabha Atomic Research Centre for all preprints and reprints of publications related to plutonium. The center wanted to include this information in a quarterly entitled Plutonium Briefs, which the center began publishing in October 1984. The letter also stated that the center tried to include all aspects of plutonium chemistry and technology in the quarterly and was interested in obtaining the names of individuals who might be interested in receiving it. According to a DOE document, the center requested this data so that it could expand the information it had already received.

In a second example, a Pakistani, who had been assigned to Los Alamos and then returned to his country, requested a document by title and publication from the laboratory. The document provided information on methods to shape plutonium metal. According to a DOE document, the report had originally been classified and could "obviously" have nuclear weapons applications. In this case, the Los Alamos employee handling the request contacted DOE headquarters officials. The officials recommended that the report be withheld. However, DOE documents state that the report would have been sent but for the employee's curiosity.

DOE does not require the laboratories to maintain information on direct requests. However, in 1986 Defense Programs provided funding to

Sandia to develop a system to track such requests and conduct technology transfer analyses. The system includes information about the document requested and response date, the name and country of the requester, and key words from the document. In addition, at Defense Programs request Sandia required that all requests for technical information from communist and other sensitive countries be reviewed by the laboratory's Technology Transfer and Management Department prior to being sent. As a result, this office, not the individual, decides whether the information should be provided.

Neither Livermore nor Los Alamos has developed a system as extensive as Sandia's. Livermore attempts to track direct requests but relies on laboratory officials to report all such contacts. In addition, at Livermore the report's author decides whether the information should be provided. However, in August 1988 Los Alamos began collecting and providing Sandia information on direct requests and implemented a system whereby its Communications and Records Management Division reviews all requests before any documents are sent. Since taking these actions, Los Alamos has received an average of about 400 direct requests each month.

Between October 1985 and December 1987, Livermore recorded about 680 direct requests, Sandia recorded about 1,360, and Los Alamos recorded 5 direct requests, including a computer code that was sent to Poland, from foreign nationals to laboratory staff. Table 2.3 shows the number of requests for information from communist countries recorded by the three weapons laboratories between October 1985 and December 1987.

Table 2.3: Requests for Information From Communist Countries—October 1985 to December 1987

Laboratory	Number requested	Number sent	Number not sent
Sandia[a]	971	903	68
Los Alamos	5	5	•
Livermore	438	276	162
Total	**1,414**	**1,184**	**230**

[a]According to a laboratory official, Sandia's data for 1986 may not be complete.

The top three recipient countries, according to available documentation, were East Germany (346), Czechoslovakia (226), and Poland (186).

In addition, sensitive countries such as Argentina, India, and Israel contact the laboratories for information. Table 2.4 shows requests from these and other sensitive countries.

Table 2.4: Requests for Information From Other Sensitive Countries—October 1985 to December 1987

Laboratory	Number requested	Number sent	Number not sent
Sandia[a]	388	351	37
Los Alamos[b]	•	•	•
Livermore	239	133	106
Total	**627**	**484**	**143**

[a]According to a laboratory official, Sandia's data for 1986 may not be complete.

[b]Los Alamos did not maintain this information until August 1988.

As shown in tables 2.3 and 2.4, the laboratories did not provide all the information requested. Livermore did not honor 268 (162 from communist and 106 from other sensitive countries) requests. Of these, it referred 60 to OSTI or NTIS and denied the remainder primarily because the laboratory had no record of the report requested. In addition, Sandia did not honor 105 requests (68 from communist and 37 from other sensitive countries) for various reasons, such as the report had a limited distribution restriction, had not yet been published, or the laboratory had no record of it.

Conferences Provide Contacts

DOE recognizes that conferences and symposia provide opportunities for foreign nationals to approach laboratory personnel and obtain information. DOE has recognized the need to continually sensitize laboratory personnel to the potential threats posed by conferences. In this regard, in 1987 DOE began nonproliferation awareness meetings at the laboratories. According to Defense Programs officials, the laboratories' response to these voluntary meetings has varied. For example, meetings held in 1988 at Sandia and Los Alamos were well attended, but one at Livermore was not. However, meetings held in January 1989 were well attended by Livermore and Sandia, but not at Los Alamos.

Dual-Use Hardware Exported to Sensitive Countries

Countries suspected of developing or enhancing their nuclear weapons capabilities routinely obtain dual-use hardware from the United States. In calendar year 1987, for example, 12 sensitive countries submitted about 1,160 export requests for more than 65,000 dual-use items in 8 categories, including digital oscilloscopes, neutron generators, flash x-

ray systems, and special cameras. Commerce approved all but 23 (about 10,420 items) of the export requests. In addition, we found that at least 290 of the approved requests were for items to be provided to organizations or facilities that are, have been, or could be assisting unsafeguarded nuclear facilities—including those involved with weapons development. According to Defense Programs officials, although DOE is required to review nuclear-related export requests, Commerce does not have to follow DOE's recommendation to deny an export license request.

Although many of the items have commercial uses and most of the export requests stated those purposes, we found that four countries received hardware that would benefit their weapons development activities. In addition, a foreign company obtained a neutron generator that uses a tritium-deuterium reaction to produce neutrons; available documentation shows that the company planned to use this equipment for oil field servicing. According to Los Alamos and Sandia officials, a company could adapt some of the hardware for nuclear weapons use. Defense Programs, Los Alamos, and Sandia officials told us that, because the hardware exported has many commercial uses, completely restricting their export is not feasible or practical. According to Defense Programs officials, they provide Commerce information to identify export requests that DOE must review and plan to periodically update the information to include "state-of-the-art" and emerging technologies that warrant greater scrutiny and attention before export licenses are approved.

In addition, DOE recognizes that U.S. controls are effective only when other potential suppliers cooperate in limiting the export of dual-use hardware. Currently, no multilateral program exists to control the international flow of technology that could help a proliferation-risk country design, develop, test, or manufacture a nuclear weapon. Nevertheless, DOE has been working with various international organizations, such as the International Atomic Energy Agency through the Zangger Committee, to identify and control the transfer of technology and specially designed components used to produce fissile material—enriched uranium and plutonium—that can be used in nuclear weapons. Further, the United States, along with 14 other nations on the Coordinating Committee on Multilateral Export Controls, attempts to control exports to communist countries of equipment, components, material, and technology used to produce fissile material and nuclear devices.

DOE Efforts to Limit Information Dissemination

DOE has been slow to implement a 1981 legislative mandate to control the dissemination of some unclassified but potentially sensitive information—UCNI. As discussed in chapter 2, DOE publishes thousands of reports and the laboratories respond to thousands of foreign requests each year. Some of this information may have met the UCNI criteria, but DOE did not have policies in place until February 1988 for the laboratories to review and mark documents as UCNI. In addition, the policies state that Defense Programs would provide three types of guidance for the field offices and laboratories to identify UCNI. As of February 1989, Defense Programs had not completed the guidance required. As a result, Sandia and Los Alamos officials said they could not identify UCNI and may have provided this type of data to proliferation-risk countries.

Further, substantial controls exist over the private sector's dissemination and/or export of nuclear-related hardware and technical information. The same controls do not apply to DOE. In November 1988 DOE circulated a draft order for comment that would require DOE field offices and laboratories to identify and mark information that would be subject to export controls if the data had been developed by the private sector. Further, in January 1989, Defense Programs issued guidelines for the field offices and laboratories to use until a final order is approved. However, some have questioned whether DOE can withhold this information without specific statutory authority. Until DOE resolves this legal issue, Defense Programs officials could not estimate when they would complete the order.

DOE Has Not Yet Implemented UCNI Controls

Pursuant to the Atomic Energy Act, DOE's policy is to make available as much scientific and technical information as security, patent, and policy considerations permit. DOE can withhold data only if it is classified or otherwise exempt from the Freedom of Information Act.

In this regard, in December 1981 the Congress added section 148 to the Atomic Energy Act, which provides a Freedom of Information Act exemption for information that meets the criteria for UCNI, and established penalties of up to $100,000 for its unauthorized disclosure. The UCNI restrictions were established because of concerns over terrorist or other actions against nuclear defense facilities. Generally, UCNI prohibits the unauthorized disclosure of unclassified information related to the (1) design of nuclear defense facilities; (2) security measures for the facilities or the nuclear material in them; and (3) design, manufacture, or utilization of any nuclear weapon or component. However, DOE can prohibit the dissemination of information only if the release would

result in a significant adverse effect on public health and safety or national defense. According to Defense Programs officials, UCNI provides only very narrowly focused information controls.

In April 1983, DOE published proposed UCNI regulations in the Federal Register; DOE received written and oral comments from 176 sources. On the basis of the comments received, DOE revised the proposed regulations and published them in August 1984. On April 22, 1985, DOE issued the final UCNI regulations (10 C.F.R. Part 1017), which in part exempted UCNI from Freedom of Information Act requests. In February 1988—6 years after passage of the act and nearly 3 years after the regulations were issued—DOE issued Orders 5635.4 and 5650.3 establishing policies and procedures to identify, review, and mark documents containing UCNI. According to Defense Programs officials, in the intervening years they took a number of actions, such as providing interim guidance to the field offices and laboratories.

To fully implement UCNI's requirements, DOE Order 5650.3 requires Defense Programs to develop general, topical, and internal guidance. According to the order, the general guidance would identify the type of information that meets the UCNI criteria; the topical guidance would help identify UCNI in a specific technology or programmatic area; and the internal guidance would identify information of interest to a particular DOE office, such as Defense Programs or the laboratories. In May 1988, Defense Programs issued the general guidance; as of March 3, 1989, it had not completed the topical and internal guidance specified in the order. According to a Defense Programs official, DOE first developed the physical security guidance required by the UCNI regulations because this guidance was easier to prepare and would apply to all DOE facilities, whereas the technology guidance would primarily apply to the three weapons laboratories and entail a lengthy process to ensure that the appropriate technical areas to be controlled were identified.

However, Sandia and Los Alamos classification officials said they cannot implement UCNI without headquarters and operations office guidance. According to these officials, the May 1988 guidance is too general and raises more questions than it answers. They also pointed out that the laboratories cannot identify UCNI data and may have released this type of information to sensitive countries through direct requests, OSTI, or NTIS.

Several examples demonstrate this confusion. Last year Los Alamos published a report that discussed a particular method to recover plutonium from other chemicals. As required, Los Alamos sent the report to OSTI for distribution. Subsequently, a Sandia official reviewed the report and recommended that DOE restrict its distribution. On the other hand, Los Alamos officials argued that the report, in and of itself, did not present new information but merely summarized current techniques. Defense Programs later directed OSTI to restrict distribution. By the time it did so, copies had been distributed to about 190 locations, including 16 foreign addresses. In addition, Defense Programs now believes the report should be considered export controlled information (discussed later in this chapter); therefore, Defense Programs, Albuquerque, Los Alamos, and Sandia officials asked us not to cite the title or report number.

In a second example, Albuquerque's Director of Classification told us that the six reports obtained from NTIS by sensitive countries (see ch. 2) contain basic science information that could be helpful to proliferation-risk countries. Although the reports in and of themselves do not meet all the UCNI tests, the director said that with other data they could help a nation further its nuclear weapons activities. Others on the director's staff agree that the six reports contain only basic research information, but because of the lack of guidance, they could not reach a consensus on whether they contained UCNI. According to Defense Programs officials, they have delegated UCNI determination responsibility to the Manager, Albuquerque Operations Office, not the Director of Classification. These officials acknowledged that at other locations, such as Los Alamos, the Director of Classification has been delegated this responsibility.

DOE Recognizes Problems

In August 1987, the Acting Assistant Secretary for Defense Programs directed an in-depth study to define the scope of DOE technology innovation, transfer, and security interests. The Assistant Secretary took this action because reports had raised concerns about potential flaws in Defense Programs technology security program. In March 1988, Defense Programs published the study results, which identified a number of improvements needed to control the dissemination of unclassified sensitive information. Of the more than 15 issues raised, some of the major ones included the following:

- Total control does not appear to be feasible or desirable.
- A coherent DOE intra-agency program is needed to adequately control unclassified documents that are militarily critical.

- DOE needs to continually identify technology that should be protected from public disclosure without inhibiting technology transfer and competitiveness.
- DOE headquarters needs to provide guidance to the field offices, laboratories, and OSTI on the policies and procedures to review unclassified sensitive scientific and technical information before its release.
- Procedures for handling "Dear Colleague" requests need to be standardized and uniformly applied.
- Communist and other sensitive countries place a high degree of confidence in applying DOE-originated technology to their programs.

The study also found that, despite legislation to strengthen DOE's controls over certain unclassified information, evidence exists that significant technology leaks persist and the U.S. government has not addressed the issue of technology protection in a comprehensive and coordinated manner. To address some of the issues raised by the study, Defense Programs issued the general UCNI guidance in May 1988 and issued guidelines to limit the foreign dissemination of certain unclassified information (export controlled) in January 1989. In January 1989, the Acting Assistant Secretary for Defense Programs also asked DOE's General Counsel to determine whether certain export controlled information could be exempt from Freedom of Information Act requests.

Previously, we reported that the Department of Defense has been granted a specific legislative exemption from Freedom of Information Act requests for unclassified information with military or space applications under its control.[1] At that time, we recommended that the Secretary of Energy seek an exemption for DOE-developed information related to the reprocessing of spent reactor fuel. DOE has not implemented this recommendation.

DOE Has Developed Export Control Guidelines

The Atomic Energy and Nuclear Non-Proliferation Acts require controls over the export of some unclassified nuclear research and development results. In addition, in 1985 the Congress amended the Export Administration Act, emphasizing the need for export controls on technologies that could significantly contribute to the military potential of other countries. Therefore, if the private sector wants to export nuclear-related or militarily critical information or technology, the company must receive a license from Commerce. For nuclear-related information,

[1] Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information (GAO/RCED-87-150, Aug. 17, 1987).

DOE must determine that a proposed export is not detrimental to the interests of the United States before Commerce issues a license. In addition, the private sector itself ensures that it does not disclose information that could help competitors. Companies do not publicize their information, since the commercial value of the data is reduced, or even destroyed, if it is made available to the public.

However, DOE does not develop government-proprietary information and is required to freely disseminate all information that is not classified or otherwise controlled. Therefore, the export license requirements do not apply to DOE. The Atomic Energy Act exempts DOE from receiving prior authorization to transfer nuclear technology and information to foreign countries, except for the transfer of sensitive nuclear technology.[2] Consistent with the provisions of the act, DOE's regulations (10 C.F.R. 810) apply only to individuals and entities other than DOE.

To help prevent the inadvertent transfer of information to foreign governments, firms, or individuals and comply with the Nuclear Non-Proliferation Treaty, in November 1988 DOE circulated a draft order (5650.4) for comment that would require DOE's field offices and laboratories to identify and mark information that should be subject to controls similar to those applicable to the private sector. At Defense Programs' request, Sandia had conducted a study that found as many as 250 requests for information each week to Los Alamos that potentially could be "export controlled information." In addition, Defense Programs estimates that several thousand documents published each year could meet the export controlled criteria. Further, in January 1989 Defense Programs issued guidelines for the field offices and laboratories to use until a final order is approved.

The guidelines apply to all unclassified DOE scientific and technical information that private industry could not export without a license under the Arms Export Control, Export Administration, Atomic Energy, or Nuclear Non-Proliferation Acts. If the information could damage national security or contribute to nuclear proliferation by improving a country's ability to build and operate certain facilities, such as enrichment or reprocessing plants, or develop nuclear weapons or naval propulsion, the guidelines state that the data should be designated export

[2]Sensitive nuclear technology is information that is not Restricted Data, is not publicly available, and is important to the design, construction, operation, or maintenance of a reprocessing, enrichment, or heavy water production facility.

controlled information and dissemination to foreign countries should be avoided.

The areas of concern include technologies pertinent to nuclear proliferation and national defense, as set out in the legislatively mandated Militarily Critical Technologies List. The guidelines specify four nuclear-related information categories—materials, reactors, weapons, and inertial fusion technologies—and lists 10 sensitive, nonnuclear technologies that should be reviewed to determine whether limited distribution is warranted. However, export controlled information would not be exempt from Freedom of Information Act requests. According to a Defense Programs study, the release of such information into the public domain automatically results in uncontrolled foreign access.

To ensure that information identified in the guidelines is not sent overseas, DOE's program offices, field offices, and laboratories must review the information. According to the guidelines, if these offices determine that the information should be controlled and only released domestically, then the release should be handled through existing distribution channels and cannot be sent to a foreign national or country unless authorized by the appropriate headquarters program office.

In addition, in August 1987 and June 1988 the Acting Secretary for Defense Programs sent a memorandum to DOE's field offices and three weapons laboratories stressing the need to evaluate the national security implications of distributing computer codes that have dual use or economic value. To strengthen this practice, the guidelines—within the nuclear weapons technology category—address the need to review computer codes to ensure they do not meet the criteria for export controlled information. In particular, the guidelines specify that codes developed for inertial fusion, reactor safety, or astrophysics should be carefully reviewed prior to being made publicly available.

However, some within DOE have questioned whether the agency can institute export controls without specific legislative authority to do so. According to Defense Program officials and a January 12, 1989, memorandum from the Acting Assistant Secretary for Defense Programs to DOE's General Counsel, two reasons exist for the agency's taking this action.

- Article I of the Nuclear Non-Proliferation Treaty commits signatories not to directly or indirectly assist non-weapons states develop nuclear explosive devices.

- The guidelines include all nuclear proliferation and national defense technologies identified in the Militarily Critical Technologies List.

Therefore, the guidelines are intended to meet the U.S. commitment under the Nuclear Non-Proliferation Treaty and comply with the Export Administration Act's requirements concerning militarily critical exports. In addition, since the Department of Defense was granted a Freedom of Information Act exemption for sensitive unclassified information related to military or space applications, Defense Programs officials believe a precedent exists for DOE to seek a similar exemption. As a result, on January 12, 1989, the Acting Assistant Secretary requested DOE's General Counsel to seek a Freedom of Information Act exemption for unclassified export controlled data that has military or space applications. The Acting Assistant Secretary pointed out that without an exemption DOE "will be" releasing information comparable to data that Defense is authorized to withhold.

Until the questions of whether DOE needs statutory authority to withhold export controlled information are resolved, Defense Programs officials could not estimate when they would complete the export control order. In addition, according to DOE's Deputy General Counsel for Programs, he expects to respond to Defense Programs' request in July 1989. The Deputy General Counsel did not believe he should speculate about the outcome at this time.

Conclusions and Recommendations

Free Flow of Information May Endanger National Security

DOE faces a dilemma because it must balance the conflicting objectives of controlling yet disseminating unclassified nuclear information and technology. For more than 40 years, DOE has designed, produced, and tested nuclear weapons and has a vast store of proven technical experience and information that could be useful to countries just beginning to develop or advance their nuclear weapons efforts. Although DOE limits the distribution of classified information, unclassified research results are widely disseminated with little or no restrictions. Some want DOE to publish as much data as possible to facilitate scientific understanding and allow the widespread dissemination of technological advances. Others believe that information dissemination needs to be restricted because some data have nuclear weapons as well as commercial applications.

With India's explosion of a peaceful nuclear device in 1974, the Congress and DOE recognized the inadequacy of many existing controls to curb nuclear proliferation. Many experts believe that the United States indirectly assisted India through the liberal publication of unclassified reprocessing information. With the passage of the Nuclear Non-Proliferation Act of 1978 and the Atomic Energy Act Amendments of 1981, the Congress expressed its concern over the potential benefit that DOE conveys to high-proliferation-risk countries through the publication of unclassified information originating from its nuclear weapons facilities. DOE's continuing to permit the free flow of information may be endangering national security and raises questions about the consistency of DOE's actions with this country's nonproliferation policy. This policy prohibits direct or indirect assistance to countries in the development of nuclear weapons.

DOE disseminates unclassified information through OSTI, NTIS, and NESC. NTIS and NESC records confirm that foreign countries—including those considered a security risk by DOE—obtain unclassified but potentially sensitive information developed by the weapons laboratories. Although we could not determine whether DOE's information has been used to help a country develop nuclear weapons, weaknesses exist in three areas that raise questions about DOE's ability to effectively protect national security and meet this country's nonproliferation policies.

Program Weaknesses

First, DOE does not require the weapons laboratories to track requests for information from foreign nationals, even though thousands of reports have been provided to these individuals each year. Many requests are from individuals in countries suspected of developing

nuclear weapons. Only Sandia has a system to monitor requests from sensitive countries; however, the system has been in place for a short time. Although Los Alamos recently began to provide information on direct requests to Sandia, without a similar system for Livermore and possibly the entire defense complex, DOE has no systematic method to determine the information that may be needed or obtained by proliferation-risk countries.

Second, contrary to DOE's policies, the weapons laboratories do not send all computer codes to NESC for distribution. NESC not only limits distribution of the codes for 2 years to give U.S. industry a competitive advantage but also flags requests from sensitive countries for Defense Programs. This office assesses each such request in light of the country's proliferation status and the possible benefit that the code could provide toward furthering that status. On the other hand, the laboratories have provided the codes to foreign requesters without systematically considering the proliferation and/or national security implications of doing so.

Third, DOE has not completely implemented congressionally mandated controls to safeguard certain sensitive, unclassified information. In 1981 the Congress charged DOE to limit the dissemination of UCNI. By mid-1988 DOE had finalized its policies and general guidance, but it has not issued other guidance to the field offices or laboratories to implement the policies established.

Conclusions

The widespread dissemination of unclassified but sensitive information and technology related to atomic defense activities creates concerns because it does not provide the United States assurance that the data we develop is used only to help (1) our nuclear program; (2) the nuclear programs of countries that we have decided, as a matter of national policy, to assist; or (3) U.S. industry increase trade in nonweapons technology. We recognize that much important information and technology exists and has been made available here and in other countries. We also recognize that DOE is required to advance scientific and technological know-how by disseminating new unclassified data. Although DOE and the weapons laboratories disagree about the significance of the new data released each year, some of the information has a potentially more dangerous side—nuclear weapons applications. Therefore, unless carefully controlled, the information and technology could help proliferation-risk countries undertake or advance their weapons development activities.

With passage of the UCNI amendments in 1981, the Congress recognized the need to limit the dissemination of some unclassified information. UCNI's requirements provide only limited controls and do not fully ensure that foreign countries do not obtain sensitive information. In an effort to provide greater assurance, DOE's Office of Defense Programs has issued guidelines asking DOE's field offices and laboratories to identify information that—if it had been developed by the private sector—would be subject to export controls. However, the guidelines do not exempt export controlled data from Freedom of Information Act requests, and some within the agency have questioned DOE's authority to withhold such information without specific legislative authority to do so. Recognizing this, Defense Programs has asked DOE's General Counsel to seek a Freedom of Information Act exemption for information designated as export controlled by DOE, but no certainty exists that DOE will do so. In the interim, DOE will be providing such information to anyone—domestic or foreign—who requests it.

DOE's obtaining an exemption to the Freedom of Information Act for export controlled information would, in our opinion, resolve these questions and provide considerable benefits to the United States' nonproliferation efforts. If the Congress provides an exemption, DOE would reduce the likelihood of any indirect assistance to countries that pose a nuclear weapons proliferation risk and remove the inconsistency between the controls over DOE's dissemination of information and the controls placed on other agencies' and private-sector's activities. Although we anticipate that some in DOE and others may raise concerns over any limitation on the free dissemination of unclassified information, we believe that little overall detriment to the U.S. nuclear program or scientific and technological advancement would occur from carefully limiting the dissemination of unclassified but sensitive data. DOE could still provide information and computer codes to U.S. industry but limit foreign dissemination of them.

Recommendations to the Secretary of Energy

To help minimize the risks associated with the free dissemination of unclassified but sensitive nuclear-related information and better protect national security, we recommend that the Secretary of Energy

- require the laboratories to track foreign requests for information and institute an effective oversight measure to ensure that they do so;

- complete and issue guidance to the weapons laboratories for use in identifying and limiting the dissemination of UCNI in accordance with the 1981 congressional mandate;
- require the laboratories to send, and refer requests for, all computer codes to NESC; and
- seek a legislative exemption from the Freedom of Information Act for unclassified data categorized by DOE as export controlled information.

BLANK PAGE

Appendix I

Activities Conducted at DOE's Nuclear Weapons Laboratories

Los Alamos National Laboratory

Los Alamos National Laboratory was established in 1943 by the U.S. Army's Manhattan Engineering District to develop the first atomic bomb. The laboratory is located in Los Alamos, New Mexico, and is operated under contract by the University of California. DOE's Albuquerque Operations Office administers the contract. Although the primary mission of the laboratory continues to be designing and developing nuclear weapons, the laboratory also performs research into the peaceful uses of atomic energy, including nuclear power production and power sources for space systems.

Lawrence Livermore National Laboratory

The University of California operates the Lawrence Livermore National Laboratory, California, for DOE. The contract is administered by the San Francisco Operations Office. Nuclear weapons research and development are the prime functions of the laboratory. Livermore is also the lead laboratory for the development of lasers for the inertial confinement fusion process, with additional programs in magnetic fusion research, laser isotope separation, and nonnuclear energy research and development.

Sandia National Laboratories

The Sandia National Laboratories are operated by the American Telephone and Telegraph Company for DOE under a no-profit, no-fee contract, which is administered by DOE's Albuquerque Operations Office. Sandia consists of headquarters facilities in Albuquerque, New Mexico; a laboratory in Livermore, California; and the Tonopah Test Range in Nevada. Sandia conducts research on the development and assembly of nuclear weapons systems, nonnuclear components design and development, field and laboratory testing, manufacturing, ordnance engineering, quality assurance, stockpile surveillance, and military training. In addition, Sandia is the lead laboratory for the development of particle beams for the inertial confinement fusion process, with additional programs in solar power research and radioactive waste management projects.

Major Contributors to This Report

Resources, Community, and Economic Development Division, Washington, D.C.	Keith O. Fultz, Director, Energy Issues, (202) 275-1441 Mary Ann Kruslicky, Assistant Director
Denver Regional Office	John D. Gentry, Regional Management Representative Craig D. Richards, Regional Assignment Manager Emmanuel S. Olona, Site Senior Pamela J. Timmerman, Evaluator

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202 275 6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25 percent discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.